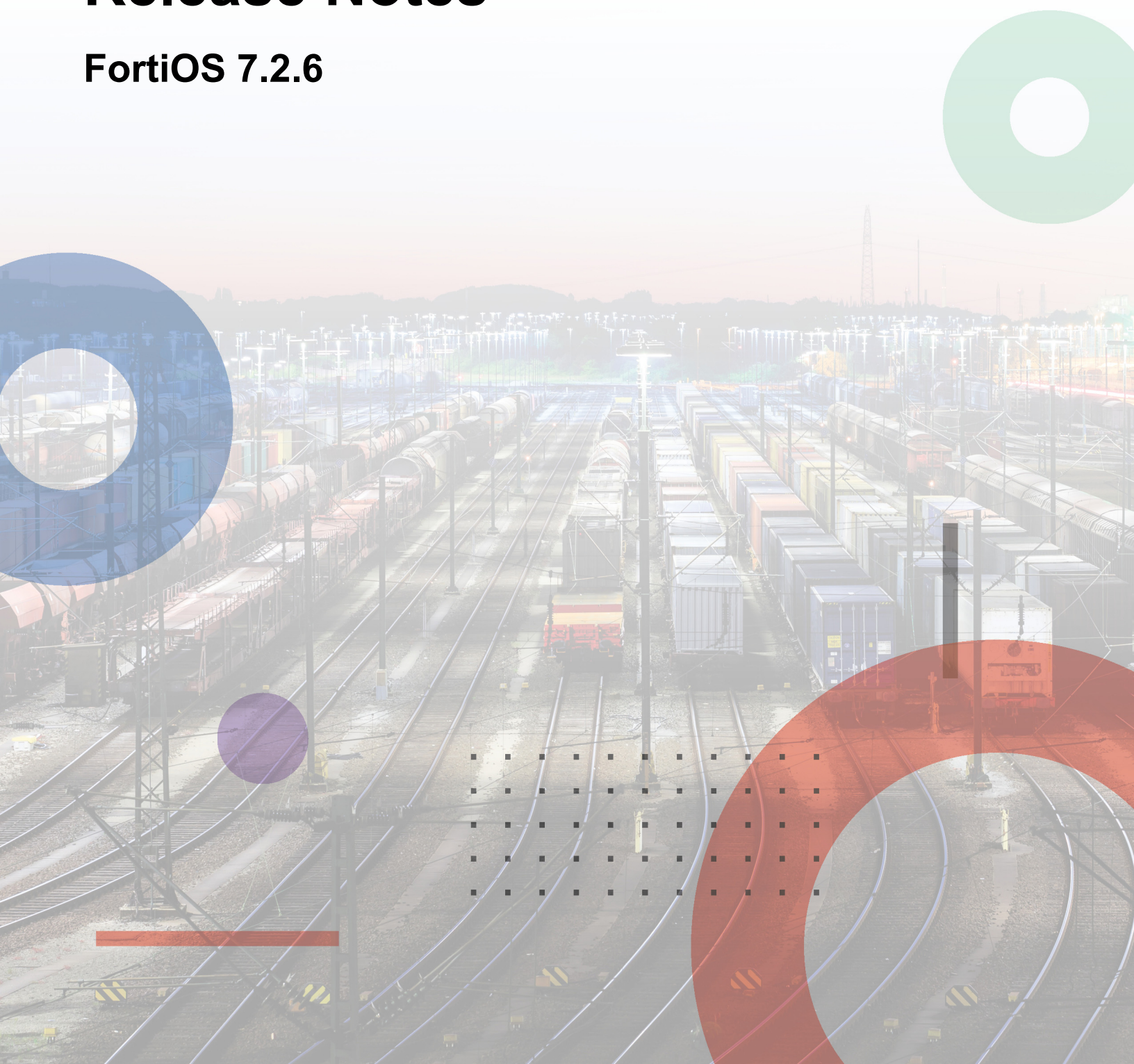
FORTINET

Release Notes

FortiOS 7.2.6



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 28, 2023
FortiOS 7.2.6 Release Notes
01-726-951004-20230928

TABLE OF CONTENTS

Change Log **5**
Introduction and supported models **6**
Supported models 6
FortiGate 6000 and 7000 support 6
Special notices **7**
IPsec phase 1 interface type cannot be changed after it is configured 7
FortiGate 6000 and 7000 incompatibilities and limitations 7
Hyperscale incompatibilities and limitations 7
Remove support for SHA-1 certificate used for web management interface (GUI) 8
SMB drive mapping with ZTNA access proxy 8
FortiGate models with 2 GB RAM cannot be a Security Fabric root 8
Console error message when FortiGate 40xF boots **10**
Changes in CLI **11**
Changes in default behavior **12**
Changes in table size **13**
New features or enhancements **14**
Upgrade information **16**
Fortinet Security Fabric upgrade 16
Downgrading to previous firmware versions 17
Firmware image checksums 18
Strong cryptographic cipher requirements for FortiAP 18
FortiGate VM VDOM licenses 18
VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name 18
FortiGate 6000 and 7000 upgrade information 19
IPS-based and voipd-based VoIP profiles 20
Upgrade error message 21
Product integration and support **22**
Virtualization environments 23
Language support 23
SSL VPN support 24
SSL VPN web mode 24
Resolved issues **25**
Anti Spam 25
Anti Virus 25
Application Control 25
Endpoint Control 26
Explicit Proxy 26
Firewall 26
FortiGate 6000 and 7000 platforms 27

FortiView 28
GUI 28
HA 29
Hyperscale 30
Intrusion Prevention 31
IPsec VPN 31
Log & Report 32
Proxy 32
REST API 33
Routing 33
Security Fabric 34
SSL VPN 35
Switch Controller 36
System 37
User & Authentication 40
VM 41
VoIP 41
Web Application Firewall 41
Web Filter 42
WiFi Controller 42
ZTNA 43
Common Vulnerabilities and Exposures 43
Known issues 44
Explicit Proxy 44
FortiGate 6000 and 7000 platforms 44
GUI 46
Hyperscale 46
IPsec VPN 46
Log & Report 47
Proxy 47
Routing 47
SSL VPN 47
System 47
Upgrade 48
Web Filter 48
WiFi Controller 48
Limitations 49
Citrix XenServer limitations 49
Open source XenServer limitations 49

Change Log

Date	Change Description
2023-09-28	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.2.6 build 1575.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.2.6 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-401E, FG-400F, FG-401F, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1000F, FG-1001F, FG-1100E, FG-1101E, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3200F, FG-3201F, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3700F, FG-3701F, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-4800F, FG-4801F, FG-5001E, FG-5001E1, FG-6000F, FG-7000E, FG-7000F
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-AZURE, FG-ARM64-GCP, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

FortiGate 6000 and 7000 support

FortiOS 7.2.6 supports the following FG-6000F, FG-7000E, and FG-7000F models:

FG-6000F	FG-6300F, FG-6301F, FG-6500F, FG-6501F
FG-7000E	FG-7030E, FG-7040E, FG-7060E
FG-7000F	FG-7081F, FG-7121F

Special notices

- IPsec phase 1 interface type cannot be changed after it is configured on page 7
- FortiGate 6000 and 7000 incompatibilities and limitations on page 7
- Hyperscale incompatibilities and limitations on page 7
- Remove support for SHA-1 certificate used for web management interface (GUI) on page 8
- SMB drive mapping with ZTNA access proxy on page 8
- FortiGate models with 2 GB RAM cannot be a Security Fabric root on page 8
- Console error message when FortiGate 40xF boots on page 10

IPsec phase 1 interface type cannot be changed after it is configured

In FortiOS 7.2.0 and later, the IPsec phase 1 interface type cannot be changed after it is configured. This is due to the tunnel ID parameter (`tun_id`), which is used to match routes to IPsec tunnels to forward traffic. If the IPsec phase 1 interface type needs to be changed, a new interface must be configured.

FortiGate 6000 and 7000 incompatibilities and limitations

See the following links for information about FortiGate 6000 and 7000 limitations and incompatibilities with FortiOS 7.2.6 features.

- FortiGate 6000 incompatibilities and limitations
- FortiGate 7000E incompatibilities and limitations
- FortiGate 7000F incompatibilities and limitations

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.2.6 features.

Remove support for SHA-1 certificate used for web management interface (GUI)

Starting in FortiOS 7.2.5, users should use the built-in Fortinet_GUI_Server certificate or SHA-256 and higher certificates for the web management interface. For example:

```
config system global
    set admin-server-cert Fortinet_GUI_Server
end
```

SMB drive mapping with ZTNA access proxy

In FortiOS 7.2.5 and later, SMB drive mapping on a Windows PC made through a ZTNA access proxy becomes inaccessible after the PC reboots when access proxy with TCP forwarding is configured as FQDN. When configured with an IP for SMB traffic, same issue is not observed.

One way to solve the issue is to enter the credentials into Windows Credential Manager in the form of `domain\username`.

Another way to solve the issue is to leverage the KDC proxy to issue a TGT (Kerberos) ticket for the remote user. See ZTNA access proxy with KDC to access shared drives for more information. This way, there is no reply in Credential Manager anymore, and the user is authenticated against the DC.

FortiGate models with 2 GB RAM cannot be a Security Fabric root

A Security Fabric topology is a tree topology consisting of a FortiGate root device and downstream devices within the mid-tier part of the tree or downstream (leaf) devices at the lowest point of the tree.

As part of improvements to reducing memory usage on FortiGate models with 2 GB RAM, this version of FortiOS no longer allows these models to be the root of the Security Fabric topology or any mid-tier part of the topology. Therefore, FortiGate models with 2 GB RAM can only be a downstream device in a Security Fabric or a standalone device.

The affected models are the FortiGate 40F, 60E, and 60F series devices and their variants.

To confirm if your FortiGate model has 2 GB RAM, enter `diagnose hardware sysinfo conserve` in the CLI and check that the total RAM value is below 2000 MB (1000 MB = 1 GB).

In the GUI on the *Security Fabric* > *Fabric Connectors* page when editing the *Security Fabric Setup* card, the *Security Fabric role* can only be configured as *Standalone* or *Join Existing Fabric*.

In the CLI, the following error messages are displayed when attempting to configure a FortiGate model with 2 GB RAM as a Security Fabric root:

```
config system csf
    set status enable
end

...
```

```
2GB-RAM models cannot be a Security Fabric root.
Please set the upstream.
object set operator error, -39, roll back the setting
Command fail. Return code -39
```

Console error message when FortiGate 40xF boots

FortiGate 40xF devices with BIOS 06000100 show an error message in the console when booting up. The message *Write I2C bus:3 addr:0xe2 reg:0x00 data:0x00 ret:-121.* is shown in the console, and the FortiGate is unable to get transceiver information.

The issue is fixed in BIOS version 06000101.

Changes in CLI

Bug ID	Description
913040	The `config vpn ssl settings` option `tunnel-addr-assigned-method` is now available again in the FortiGate 6000 and 7000 CLI. This option had been removed in a previous release because setting this option to `first-available` and configuring multiple IP pools was found to reduce FortiGate 6000 and 7000 SSL VPN load balancing performance. However, some users may want the ability to use multiple IP pools for their SSL VPN configuration, even if performance is reduced. So the change has been reverted.

Changes in default behavior

Bug ID	Description

864035	When the `auto-firmware-upgrade` setting is enabled, the FortiGate checks for updates every day between the firmware upgrade time interval. When a newer firmware is found, the installation is scheduled after the upgrade delay in days (0-14, default = 3) between the firmware upgrade time interval. After a successful update, an email is sent to the account owner.
	`config system fortiguard`
	`set auto-firmware-upgrade {enable | disable}`
	`set auto-firmware-upgrade-delay <integer>`
	`end`
	Where:
	• `auto-firmware-upgrade` is enabled by default upon upgrade.
	• `auto-firmware-upgrade-delay` is set to 3 days by default.
	Affected platforms:
	FGT-40F, FGT-40F-3G4G, FGT-60E, FGT-60E-DSL, FGT-60E-DSLJ, FGT-60E-POE, FGT-60F, FGT-61E, FGT-61F, FGT-70F, FGT-71F, FGT-80E, FGT-80E-POE, FGT-80F, FGT-80F-BP, FGT-80F-POE, FGT-81E, FGT-81E-POE, FGT-81F, FGT-81F-POE, FGT-90E, FGT-91E, FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G, FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE

930122	Automatic firmware upgrades are now enabled by default on desktop-level FortiGates (100 series and lower). Upgrades will be made to the next stable patch. However, if a FortiGate is part of a Fabric or managed by FortiManager, the `Automatic image upgrade` option is disabled.

Changes in table size

Bug ID	Description
858877	Increase the number of supported dynamic FSSO IP addresses from 100 to 3000 per dynamic FSSO group. The dynamic FSSO type addresses can be pointed to FortiManager's Universal Connector, which imports the addresses from Cisco ACI or Guardicore Centra.
891426	Table size expansion for VM04 and higher models: The Geneve Table size has been expanded to 1024 entries, and the Virtual-wire-pair table size has been increased to 512 entries. This enhancement provides greater flexibility and scalability for network configurations.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description

814242	The FortiGate 7000F platform supports setting a custom load balancing method for an individual VDOM. All of the traffic destined for that VDOM will be distributed to FPMs by the NP7 load balancers according to the following setting:
	`config system settings`
	`set dp-load-distribution-method {derived | to-master | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-ip-dport | src-dst-ip-sport-dport}`
	`end`
	The default load balancing method, `derived`, means traffic for that VDOM uses the global load balancing method set by the `dp-load-distribution-method` option of the global `config load-balance` setting command.

834861	Add route tags to static routes.
	`config router static`
	`edit <seq-num>`
	`set tag <id>`
	`next`
	`end`
	Add password field to BGP neighbor group to be used for the neighbor range.
	`config router bgp`
	`config neighbor-group`
	`edit <name>`
	`set password <password>`
	`next`
	`end`
	`end`

864021	Introduction of a new Firmware Virtual Patch (FMWP) database to support local-in virtual patching. To install the FMWP database, the FortiGate must have a valid Firmware (FMWR) license. The FMWP database can be viewed by running the `diagnose autoupdate versions` command.
875306	New command added to compute the SHA256 file hashes for each file in a directory: `# diagnose sys filesystem hash`
884772	Securely exchange serial numbers between FortiGates connected with IPsec VPN. This feature is supported in IKEv2, IKEv1 main mode, and IKEv1 aggressive mode. The exchange is only performed with participating FortiGates that have enabled the `exchange-fgt-device-id` setting under `config vpn ipsec phase1-interface`.

Feature ID	Description
897240	The Any/All GUI selector for ZTNA tags is added back to the simple and full ZTNA policy configuration page. The setting is defaulted to Any.
899827	Improve the client-side settings of the SD-WAN network bandwidth monitoring service to increase the flexibility of the speed tests, and to optimize the settings to produce more accurate measurements. The changes include: • Support UDP speed tests. • Support multiple TCP connections to the server instead of a single connection. • Measure the latency to speed test servers and select the server with the smallest latency to perform the test. • Support the auto mode speed test, which selects either UDP or TCP testing automatically based on the latency threshold.

904189	FOS can synchronize the FOS interface description with the VLAN description on the FortiSwitch. Previously, only the FOS interface name could be synchronized as the VLAN description on the FortiSwitch, and it was limited to 15 characters. This enhancement extends the VLAN description length on the FortiSwitch from 15 characters to a new maximum of 64 characters.
	CLI changes:
	`config switch-controller global`
	`  set vlan-identity {name | description}`
	`end`

909935	Include a built-in entropy token source, which eliminates the need for a physical USB entropy token when booting up in FIPS mode on any platform. This enhancement meets the requirements of FIPS 140-3 Certification by changing the source of entropy to jitter entropy, which is known for its reliability and security.
916723	Introduce compatibility between FortiGate-VM64.ovf and FortiGate-VM64.vapp.ovf templates with VMware ESXi 8, virtual hardware version 20.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Fortinet Security Fabric upgrade

FortiOS 7.2.6 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.2.3
FortiManager	• 7.2.3
FortiExtender	• 7.4.0 and later
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 18
FortiClient* EMS	• 7.0.3 build 0229 or later
FortiClient* Microsoft Windows	• 7.0.3 build 0193 or later
FortiClient* Mac OS X	• 7.0.3 build 0131 or later
FortiClient* Linux	• 7.0.3 build 0137 or later
FortiClient* iOS	• 7.0.2 build 0036 or later
FortiClient* Android	• 7.0.2 build 0031 or later
FortiSandbox	• 2.3.3 and later for post-transfer scanning • 4.2.0 and later for post-transfer and inline scanning

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.2.0, use FortiClient 7.2.0.

Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiNAC
13. FortiVoice
14. FortiDeceptor
15. FortiNDR
16. FortiTester
17. FortiMonitor
18. FortiPolicy

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.2.6. When Security Fabric is enabled in FortiOS 7.2.6, all FortiGate devices must be running FortiOS 7.2.6.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account

- session helpers
- system access profiles

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in, go to *Support* > *Firmware Image Checksums* (in the *Downloads* section), enter the image file name including the extension, and click *Get Checksum Code*.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 and later need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

FortiGate VM VDOM licenses

FortiGate VMs with one VDOM license (S-series, V-series, FortiFlex) have a maximum number or two VDOMs. An administrative type root VDOM and another traffic type VDOM are allowed in 7.2.0 and later. After upgrading to 7.2.0 and later, if the VM previously had split-task VDOMs enabled, two VDOMs are kept (the root VDOM is an administrative type).

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later

- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

FortiGate 6000 and 7000 upgrade information

Upgrade FortiGate 6000 firmware from the management board GUI or CLI. Upgrade FortiGate 7000 firmware from the primary FIM GUI or CLI. The FortiGate 6000 management board and FPCs or the FortiGate 7000 FIMs and FPMs all run the same firmware image. Upgrading the firmware copies the firmware image to all components, which then install the new firmware and restart. A FortiGate 6000 or 7000 firmware upgrade can take a few minutes, the amount of time depending on the hardware and software configuration and whether DP or NP7 processor software is also upgraded.

On a standalone FortiGate 6000 or 7000, or an HA cluster with `uninterruptible-upgrade` disabled, the firmware upgrade interrupts traffic because all components upgrade in one step. These firmware upgrades should be done during a quiet time because traffic can be interrupted for a few minutes during the upgrade process.

Fortinet recommends running a graceful firmware upgrade of a FortiGate 6000 or 7000 FGCP HA cluster by enabling `uninterruptible-upgrade` and `session-pickup`. A graceful firmware upgrade only causes minimal traffic interruption.

Fortinet recommends that you review the services provided by your FortiGate 6000 or 7000 before a firmware upgrade and then again after the upgrade to make sure that these services continue to operate normally. For example, you might want to verify that you can successfully access an important server used by your organization before the upgrade and make sure that you can still reach the server after the upgrade and performance is comparable. You can also take a snapshot of key performance indicators (for example, number of sessions, CPU usage, and memory usage) before the upgrade and verify that you see comparable performance after the upgrade.

To perform a graceful upgrade of your FortiGate 6000 or 7000 to FortiOS 7.2.6:

Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12 to 7.2.6.

Upgrading the firmware of a FortiGate-6000 or 7000 FGCP HA cluster from 7.0.12 to 7.2.6 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for a few minutes.

Before upgrading the firmware, disable `uninterruptible-upgrade`, then perform a normal firmware upgrade. During the upgrade process the FortiGates in the cluster will not allow traffic until all components (management board and FPCs or FIMs and FPMs) are upgraded and both FortiGates have restarted. This process can take a few minutes.

1. Use the following command to enable `uninterruptible-upgrade` to support HA graceful upgrade:

   ```
   config system ha
       set uninterruptible-upgrade enable
   end
   ```

2. Download the FortiOS 7.2.6 FG-6000F, FG-7000E, or FG-7000F firmware from https://support.fortinet.com.
3. Perform a normal upgrade of your HA cluster using the downloaded firmware image file.
4. When the upgrade is complete, verify that you have installed the correct firmware version.
   For example, check the FortiGate dashboard or use the `get system status` command.
5. Confirm that all components are synchronized and operating normally.
   For example, go to *Monitor* > *Configuration Sync Monitor* to view the status of all components, or use `diagnose sys confsync status` to confirm that all components are synchronized.

IPS-based and voipd-based VoIP profiles

Starting in FortiOS 7.2.5, the new IPS-based VoIP profile allows flow-based SIP to complement SIP ALG while working together. There are now two types of VoIP profiles that can be configured:

```
config voip profile
    edit <name>
        set feature-set {ips | voipd}
    next
end
```

A voipd-based VoIP profile is handled by the voipd daemon using SIP ALG inspection. This is renamed from proxy in previous FortiOS versions.

An ips-based VoIP profile is handled by the IPS daemon using flow-based SIP inspection. This is renamed from flow in previous FortiOS versions.

Both VoIP profile types can be configured at the same time on a firewall policy. For example:

```
config firewall policy
    edit 1
        set voip-profile "voip_sip_alg"
        set ips-voip-filter "voip_sip_ips"
    next
end
```

Where:

- `voip-profile` can select a `voip-profile` with `feature-set voipd`.
- `ips-voip-filter` can select a `voip-profile` with `feature-set ips`.

The VoIP profile selection within a firewall policy is restored to pre-7.0 behavior. The VoIP profile can be selected regardless of the inspection mode used in the firewall policy. The new `ips-voip-filter` setting allows users to select an IPS-based VoIP profile to apply flow-based SIP inspection, which can work concurrently with SIP ALG.

Upon upgrade, the `feature-set` setting of the `voip profile` determines whether the profile applied in the firewall policy is `voip-profile` or `ips-voip-filter`.

Before upgrade	After upgrade
config voip profile edit "ips_voip_filter" set feature-set flow next edit "sip_alg_profile" set feature-set proxy next end config firewall policy edit 1 set voip-profile "ips_voip_filter" next edit 2 set voip-profile "sip_alg_profile" next end	config voip profile edit "ips_voip_filter" set feature-set ips next edit "sip_alg_profile" set feature-set voipd next end config firewall policy edit 1 set ips-voip-filter "ips_voip_ filter" next edit 2 set voip-profile "sip_alg_profile" next end

Upgrade error message

The FortiGate console will print a `Fail to append CC_trailer.ncfg_remove_signature:error in stat` error message after upgrading from 7.2.4 to 7.2.5 or later. Affected platforms include: FFW-3980E, FFW-VM64, and FFW-VM64-KVM. A workaround is to run another upgrade to 7.2.5 or later.

Product integration and support

The following table lists FortiOS 7.2.6 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 0312 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00293
IPS Engine	• 7.00326

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0.

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 7.2.6. To inquire about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
870052	Error condition in scanunitd occurs when emailfilter-profile and proxy inspection are applied to a firewall policy.

Anti Virus

Bug ID	Description
908706	On the *Security Profiles* > *AntiVirus* page, a VDOM administrator with a custom administrator profile cannot create or modify an antivirus profile belonging to the VDOM.
911332	When UTM status is enabled and the AV profile has no configuration, all SLL traffic is dropped and there is no WAD output.
923883	The FortiGate may display an error log in the crashlog due to AV delta update. In case of failure, full successful AV update is done.

Application Control

Bug ID	Description
913529	The firewall policy dialog should show the no-inspection profile and the warning should be consistent with the policy list.
939565	`can not query meta rules list` seen on graceful/ non-graceful upgrade.

Endpoint Control

Bug ID	Description
897048	FortiOS should support EMS 7.2.1 auth API status code changes.
913324	GUI repeated calls to the EMS API, which can cause EMS to not authorize the FortiGate correctly.
933819	Two FortiGates deregistered from EMS on special build 8844.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.
859693	Session state is incorrectly shown as `SYN_SENT` when using an IP pool in explicit proxy policy.
866316	Explicit web proxy fails to forward HTTPS request to a Squid forward-server when certificate inspection is applied.
888078	Enabling `http-ip-header` on virtual server changes the log produced for transparent web proxy.
889300	Wrong source IP address used for packets through explicit proxy routed to a member of SD-WAN interface.
908989	The *Enabled On* should display the listening interface(s) rather than *None* in explicit proxy policy on the GUI.
923302	Cannot send picture through web explicit proxy.
934094	Some websites through explicit proxy randomly getting blocked after upgrade.

Firewall

Bug ID	Description
843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI. This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
872312	Unable to add more MAC addresses once the MAC address group object for a VWP policy referenced.

Bug ID	Description
879225	Egress Interface cannot be intermittently matched for Wake On LAN [broadcast] packets.
879705	Traffic issues occur with virtual servers after upgrading.
884908	Implicit deny policy is allowing "`icmp/0/0`" traffic.
895946	Access to some websites fails after upgrading to FortiOS 7.2.3 when the firewall policy is in flow-based inspection mode.
909763	Wrong TOS field value in netflow report when there is no traffic.
912089	High CPU utilization due to sflowd and no data sent to the collector.
914939	UDP fragments dropped due to DF being set. Only the `set honor-df global` option.
926029	New sessions are created and evaluated after a certain number of UDP packets, even if `set block-session-timer 300` is set.
927009	When running tests with SNAT PBA source and destination IP addresses, octets are shown on reverse order.
928896	`set fixedport enable` in a firewall policy does not preserve the source port for SNAT with ippool.

FortiGate 6000 and 7000 platforms

Bug ID	Description
758078	After system synchronization, master blades' reboot command did not take effect on the slaves.
888310	The FortiGate 6000 or 7000 front panel does not appear on the *Network* > *Interfaces* and *System* > *HA* GUI pages.
888447	In some cases, the FortiGate 7000F platform cannot correctly reassemble fragmented packets.
891430	The FortiGate 6000 and 7000 *System Information* dashboard widget incorrectly displays the management board or primary FIM serial number instead of the chassis serial number. Use `get system status` to view the chassis serial number.
891642	FortiGate 6000 and 7000 platforms do not support managing FortiSwitch devices over FortiLink.
896758	Virtual clustering is not supported by FortiGate 6000 and 7000 platforms.
897629	The FortiGate 6000 and 7000 platforms do not support EMAC VLANs.
899905	Adding a FortiAnalyzer to a FortiGate 6000 or 7000 Security Fabric configuration from the FortiOS GUI is not supported.
901695	On FortiGate 7000F platforms, NP7-offloaded UDP sessions are not affected by the `udp-idle-timer` option of the `config system global` command.
905450	SNMP walk fails to get BGP routing information.

Bug ID	Description
907140	Authenticated users are not synchronized to the secondary FortiGate 6000 or 7000 chassis when the secondary chassis joins a primary chassis to form an FGCP cluster.
908576	On a FortiGate 7000F, after a new FPM becomes the primary FPM, IPsec VPN dynamic routes are not synchronized to the new primary FPM.
908674	Sessions for IPsec dialup tunnels that are configured to be handled by a specific FPC or FPM may be incorrectly sent to a different FPC or FPM, resulting in traffic being blocked.
909160	The FortiGate 7000E and 7000F platforms do not support GTP and PFCP load balancing.
913040	Multiple IP pools in SSL VPN is not supported.
914273	SNMP query to fgVdEntSesRate returns a 0 value.
918795	An uncertified warning appears only on the secondary chassis' FIM02 and FPMs.
920925	Graceful upgrade from 7.0.12 to 7.2.5 fails sometimes due to the primary chassis not being switched over.
921452	After an SNMP HA failover, the SNMP trap continues to work.
947936	On the FortiGate 7060E, only 4 of 6 PSUs are shown sometimes.

FortiView

Bug ID	Description
894957	FortiView Websites: realtime view is always empty if disk logging disabled.
920241	GUI shows *Failed to retrieve FortiView data* while accessing *FortiView Sources* and *FortiView Destination*.
950137	Unable to see *Application* information in *FortiView Application* for the proxied traffic.

GUI

Bug ID	Description
825598	The FortiGate may display a false alarm message `TypeError [ERR_INVALID_URL]: Invalid URL` in the crashlog for the node process. This error does not affect the operation of the GUI.
863126	In an environment where the Security Fabric is enabled and there are more than 100 firewall object conflicts between the root and downstream FortiGates, the *Firewall Object Synchronization* pane does not list the details.

Bug ID	Description
892364	Incorrect interface is being selected in the *SD-WAN Rules* GUI page, but the correct one is displayed in the CLI.
893560	When private data encryption is enabled, the GUI may become unresponsive and HA may fail to synchronize the configuration.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog.
903856	When using configuration save mode with VDOMs, the GUI still shows unsaved changes after another administrator commits their changes with SSH.
904817	Each value of *IPv4*, *IPv6*, and *IPv4 + IPv6* selected on *Session Rate* is changed after returning to Status.
907041	*Network* > *SD-WAN* > *SD-WAN Zones* and *SD-WAN Rules* pages do not load if a shortcut tunnel is triggered.
919390	Disabling `gui-wireless-controller` on the root VDOM impacts other VDOMs (unable to add or show WiFi widgets on first load).
931004	FortiGate GUI issues on mobile phone's browser.
931486	GUI hangs when the administrator is switching back and forth between policy (5K) and address (8K) pages.
946116	Guest account provisioning admin on a FortiGate managed by FortiManager shows read only permission but lets them create accounts.
946878	FortiGate ha-mgmt-interface GUI not allowing multiple route entries, but the CLI does allow them.

HA

Bug ID	Description
703614	HA secondary synchronization fails and keeps rebooting when the primary has a split port configuration.
771316	Platforms in an HA environment get stuck in a reboot loop while attempting to synchronize configurations that differ in split ports.
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
870312	On a FortiGate HA cluster, both primary and secondary units are displayed as the *Primary* on the GUI top banner, and as `Current HA mode` in the CLI.
875984	FortiGate is going to out-of-sync after changing parameters of VDOM link interfaces.
880786	Running `diagnose sys ha vlan-hb-monitor` incorrectly shows inter-VDOM VLANs inactive.

Bug ID	Description
881337	Adding a VLAN interface on any VDOM causes BGP flapping and VIP connectivity issues on VDOMs in vcluster2.
881847	HA interfaces flapping on FG-3401E.
883546	In HA, sending lot of CLI configurations causes the creation of a VDOM on the secondary unit.
888110	Unable to set the interface configured as an SD-WAN member to `pingserver-monitor-interface` in the CLI.
893041	Cannot access out-of-band ipv6 address on HA secondary unit.
896608	HA cluster became out-of-sync after enabling a password policy and logging on to FortiGate.
897865	When NP7 platforms enable the GTP enhanced mode it does not use uninterruptible upgrade.
901292	When entering the psksecret under `config system standalone-cluster`, no verifications are done against the password-policy ipsec-preshared-key.
902945	Lost management connectivity to the standby node via in-band management.
904318	FortiGate sent ARP request with loopback IP address as source the address.
906367	Upgrading a cluster of four FortiGate 2200E devices, each secondary forms a cluster with the primary only and causes an outage.
908062	FortiGate VM Azure HA cluster goes out-of-sync due to dynamic firewall address type.
916216	When adding a new interface, some other interface has the wrong virtual MAC address.
916903, 919982, 922867	When an HA management interface is configured, the GUI may not show the last interface entry in `config system interface` on several pages, such as the interface list, policy list, address list, and DNS servers page. This is a GUI-only display issue and does not impact the underlying operation of the affected interface.
919005	Heartbeat packet loss issue at random times.
920233	The *System* > *HA* page is missing from the GUI on 5K models.
931724	HA events not synchronizing between members, leading to unexpected HA status.
935448	Hardware session synchronization is showing out-of-sync on primary and secondary.

Hyperscale

Bug ID	Description
915796	With an enabled hyperscale license, in some cases with exception traffic (like ICMP error traverse), the FortiGate may experience unexpected disruptions when handling the exception traffic.
920405	Problem with synchronizing a high amount of routes to NP7 for Hyperscale firewall.
924196	Device is rebooting randomly when driver processes exception packets.

Bug ID	Description
932317	Hyperscale firewall creates a separate session and uses a different source port for IP fragment packets.
933063	LPM daemon is being killed.

Intrusion Prevention

Bug ID	Description
823583	Failover on clustered web application using keepalived daemon does not work seamlessly.
842523	IPv6 with hardware offloading and IPS drops traffic (`msg="anti-replay check fails, drop).`
845944	Firewall policy change causes high CPU spike with IPS engine.
860315	Unexpected behavior in IPSengine when executing `diagnose test application ipsmonitor 44`.
873975	Source MAC changes and the packet drops due to both sides of the session using the same source MAC address.
874877	IPSengines do not release memory after stopping traffic more than 1 hour.
886685	IPS daemon usage issue when notifying device vulnerability information to WAD.
892302	Constant reloading of the external domain table is causing high CPU due to lock contention when reloading the table.
926639	Constant reloading of the shared memory external domain table is causing high CPU usage due to lock contention when reloading the table.
934015	RSH subsession timeout when IPS is enabled.

IPsec VPN

Bug ID	Description
803010	The `vpn-id-ipip` encapsulated IPsec tunnel with NPU offloading cannot be reached by IPv6.
872769	Proxy ARP stops working for a client connected to a dialup IPsec when the previous VPN was established and is deleted.
883138	VM running FIPS cipher mode does not show AES-CBC ciphers when configuring IPsec in the GUI.
885333	Forwarded broadcast traffic on ADVPN shortcut tunnel interface dropped.
898872	IPsec performance drops after upgrade on AWS.

Bug ID	Description
914418	File transfer stops after a while when offloading is enabled.
926048	Traffic through a shortcut got dropped after an HA failover.
928774	IPsec VPN connection should allow % in FortiClient Connect REG_PASSWD field.

Log & Report

Bug ID	Description
831441	The forward traffic log show exabytes of data being sent and received from external to external IP addresses in multiple VDOMs.
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries.
861893	In *Forward Traffic* logs, the *Policy ID* column is blank.
865794	Log Viewer: filter by Date/Time does not show correct result.
879446	`diagnose sys logdisk smart` does not work for NVME disk models.
893199	The FortiGate does not generate deallocate/allocate logs of the first IP pool when the first IP pool has been exhausted.
902797	IPS alert email not being sent when IPS attack event has triggered.
908856	Traffic log can show exabytes of data sent and received when generating log task is triggered from userspace.
929338	Secondary FortiGate log cannot be viewed from primary FortiGate in HA.
932817	Forward traffic log has unexpected symbols in the end for some logs.
940814	Events Log view menu is not showing up with custom admin profile without Threat Weight option.

Proxy

Bug ID	Description
783549	An error condition occurs in WAD caused by multiple outstanding requests sent from client to server with UTM enabled.
820096	CPU usage issue in Proxyd caused by the absence of TCP Teardown.
882182	Unexpected behavior in WAD due to the activation of firewall protocol options with both client and server comfort features enabled.

Bug ID	Description
883504	Emails are blocked when proxy-based policy with either AntiVirus or Email Filter security profiles enabled.
897347	Memory leak observed for WAD user-info process.
898016	Kerberos authentication stops working after the upgrading to 7.2.3.
899358	Proxy-based deep-inspection connection issue.
902613	WAD crash during stress testing.
904386	Unable to upload file to the application server in server-load-balance setup.
921247	WAD worker consuming high memory and CPU.
932487	WAD worker memory usage slowly increases.

REST API

Bug ID	Description
948356	An error condition occurs in HTTPSD when a REST API request is sent with invalid parameters.

Routing

Bug ID	Description
775752	`link-down-failover` does not bring the BGP peering down.
820407	SYS:Auto Link fail if the FortiGate device initiating the FGFM connection is using an interface with VRF not set to the default 0.
858248	OSPF summary address for route redistribution from static route via IPsec VPN always persists.
858299	Redistributed BGP routes to the OSPF change its forward address to the tunnel ID.
875668	SD-WAN SLA log information has incorrect inbound and outbound bandwidth values.
892704	SD-WAN performance SLA statistics on secondary unit's GUI section are not synchronized with the primary and has stale data.
899827	Speed test result is not accurate.
900226	High CPU due to PIMD/NSM and multicast session not being offloaded.
900770	DHCP relay fails after a period of time with SDWAN.
900941	`config redistribute` routing sub-sections cannot be configured when in Workspace mode.

Bug ID	Description
907386	BGP neighbor group configured with password is not working as expected.
909835	Search broken on SD-WAN Rules > Source/Destination omniselect.
913338	FortiGate removing SD-WAN routes when network address is specified as the gateway of an SD-WAN member.
914497	SD-WAN rules list on GUI should show interface members in priority order instead of alphabetical order.
914815	FortiGate 40F-3G4G not adding LTE dynamic route to route table.
922491	Static routes installed on hub FortiGate with add-route disabled in ADVPN scenario.
924598	The *Network* dashboard may not load if the administrator disables *SD-WAN Interface* under *System > Feature Visibility*.
924940	When there are a lot of policies (several thousands), the interface member selection for the *SD-WAN Zone* dialog may take up to a minute to load.

Security Fabric

Bug ID	Description
831311	When using automation email action to reference the result of a previously executed automation cli-script action, there is a 16 kb size limit for the script output.
874822	In a configuration with a connected FortiAP-U, the *FortiAP & FortiAP-S & FortiAP-W2 & FortiAP-U Command Injection in CLI* security rating test fails and suggests an upgrade to 7.0.4, even though the FortiAP is on the latest version (7.0.0).
907819	Advanced GCP connector does not resolve if one element does not exists.
912592	Allow comments and IP addresses to be on the same line for external IP address threat feeds.
912917	Send fabric API calls with pagination filter.
917024	Unexpected behavior in Security Fabric daemon (CSFD) caused by triggering HA failover while using security fabric.
918230	Threat Feeds with name starting with 'g-' are not allowed on non VDOM FortiGate.
922896	Azure SDN connector always use HA MGMT port for DNS resolve. This might not work on premises where the HA MGMT port does not have public IP address assigned.
926202	Unable to authorize downstream FortiGate with the Security Fabric after upgrade.

SSL VPN

Bug ID	Description
631809	Configuring thousands of `mac-addr-check-rule` in portal makes the CPU spike significantly if several hundreds of users are connecting to the FortiGate, thus causing SSL VPN packet drops.
833934	SSL VPN fails to connect to graph.microsoft.com when doing Azure auto login.
843756	Customer bookmark (*.tr***.pt) is not accessible when using SSL VPN web mode.
851976	PC cannot get IP from DHCP server due to `find duplicate ip` and causes the dialup SSL VPN to fail.
856194	Problem loading some graphs trough SSL VPN web mode after upgrading.
858478	SSL VPN DTLS tunnel is unavailable after changing the SSL VPN listening port.
859088	FortiGate adds extra parenthesis and causes clicking all links to fail in SSL VPN web mode.
868491	SSL VPN web mode connection to VMware vCenter 7 is not working.
871039	Internal website is not displaying user-uploaded PDF files when visited through SSL VPN web mode.
871229	SSL VPN web mode does not load when connecting to customer's internal site.
872745	SSL VPN web mode to RDP broker leads to connection being closed.
873516	FortiGate misses the closing parenthesis when running the function to rewrite the URL.
875167	Webpage opened in SSL VPN web portal is not displayed correctly.
877124	RDP freezes in web mode with high CPU usage of SSL VPN process.
878833	Decrease in download speeds observed for SSL VPN users when over 2000 users are connected.
880791	Internal website access issue with SSL VPN web portal.
881220	Found bad login for SSL VPN web-bases access when enabling URL obscuration.
881268	Disconnecting from SSL VPN using the *SSL-VPN* widget does not disconnect the SSL VPN tunnel.
884869	Web mode bookmark showing blank page due to JS rewrite.
885978	Some buttons in URL are not working in SSL VPN Web mode.
886989	SSL VPN process reaches 99% CPU usage when HTTP back-end server resets the connection in the middle of a post request.
887345	When a user needs to enter credentials through a popup window, the key events for modification key detected by SDL were ignored.
889736	The HPE ILO 5 webserver is not able to load properly from the SSL VPN portal.
894704	FortiOS check would block IOS and Android mobile devices from connecting to the SSL VPN tunnel.
895120	SSL VPN Web portal not loading internal web page.

Bug ID	Description
896007	Specific SAP feature is not working with SSL VPN web mode.
896343	SSL VPN web mode is not working as expected for customer's web server.
896396	SSL VPN Web portal HTTP bookmark forwarded site throws Java error.
897385	Internal web site keeps asking for credential via SSL VPN Web mode.
897665	The external DHCP server is not receiving hostnames in SSL VPN and dhcprelay.
904919	DHCP option 12 hostname needed for SSL VPN with external DHCP servers.
906756	Update SSL VPN host check logic for unsupported OS.

922446	SSL VPN service over PPPoE interface does not work as expected if the PPPoE interface is configured with `config system pppoe-interface`.
	`config system pppoe-interface`
	`edit <name>`
	`set device <string>`
	`set username <string>`
	`set password <password>`
	`next`
	`end`
	
	`config vpn ssl settings`
	`set source-interface <PPPoE_interface_name>`
	`end`
	
	This issue is also observed on VNE tunnel configurations.

927475	SSL VPN tunnel-down log message not generated when an IP address is disassociated before the old tunnel times out.
933985	FortiGate as SSL VPN client does not work on NP6 and NP6xlite devices.

Switch Controller

Bug ID	Description
848632	Upon upgrade, the link to FortiSwitch stays down with QSFP.
858749	Redirected traffic should not hit the firewall policy when `allow-traffic-redirect` is enabled.
893405	One discovery one transmit buffer was allocated and was not released on connection terminations.
894735	Unable to configure more than one NAC policy using the same EMS tag for different FortiSwitch groups.
902338	*WiFi & Switch Controller* > *FortiSwitch Ports* page does not show VLANs exported to another tenant VDOM, which results in the VLAN being removed if saved from the GUI.

Bug ID	Description
904640	When a FortiSwitch port is reconfigured, the FortiGate may incorrectly retain old detected device data from the port that results in an unexpected number of detected device MACs for the port. Using `diagnose switch-controller mac-cache show` to check the device data can result in the *Device Information* column being blank on the *WiFi & Switch Controller* > *FortiSwitch Ports* page or in the *Assets* widget.
911232	Security rating shows an incorrect warning for unregistered FortiSwitches on the *WiFi & Switch Controller* > *Managed FortiSwitches*.
920231	FortiGate loses QOS ip-dscp-map configuration after reboot.
936081	`VLAN-optimization enable/disable` and `VLAN-all-mode all` configuration options disappear after upgrade/reboot.
941673	FortiSwitch event log display serial number under name when CAPWAP is up or down.

System

Bug ID	Description
631046	`diagnose sys logdisk smart` does not work for NVMe disk models.
656138	GUI shows conflicts error message when configuring a secondary IP address after `allow-subnet-overlap` enabled.
708964	CPU usage issue is observed caused by reloading the system when the system has `cfg-save` set to `revert`.
713951	Not all ports are coming up after an LAG bounce on 8 × 10 GB LAG with ASR9K. Affected platforms: FG-3960E and FG-3980E.
820559	When backing up the configuration to a USB disk, if the file name is the same as specified under *System* > *Settings* > *Start Up Settings* > *USB auto-install*, an *Invalid file name* error is displayed.
821000	QSFP and QSFP+ Fortinet transceivers are not operational on FG-3401E.
836748	FG-100F fails to boot when FortiOS image binary is larger than 94 MB.
842159	FortiGate 200F interfaces stop passing traffic after some time.
845079	DAC cable support is unstable on the FortiGate 1101E.
855573	False alarm of the PSU2 occurs with only one installed.
862519	FortiGate 40F-3G4G WWAN connection unstable on Verizon Carrier.
866437	High CPU usage by random CPU cores in system space on the FortiGate 3500F.
867663	The FEC configuration under the interface is not respected when port23 and port24 are members of an LACP and the connection is 100G. Affected platforms: FGT-340xE, FGT-360xE **Workaround**:

Bug ID	Description
	1. Take the ports out of LAG and disable FEC, and then put them back to the LAG. 2. Disable FEC manually on the driver level via commands.
869044	If the original packet was forwarded with NAT, generated ICMP error is routed back to SNAT'ed address.
869113	If a device is rebooted that has an `ipsec-STS-timeout` configured or the user configures the `ipsec-STS-timeout` before any NPU tunnel is created, NPU will send random STS messages that have an invalid tunnel index and trigger NP6XLite error messages.
869305	SNMP multicast counters are not increasing.
869726	When an IPsec tunnel is configured with a different VRF than the underlying physical interface, and traffic is offloaded, the session expires even when traffic is flowing through it.
874603	Dashboard loads slowly and csfd process has high CPU usage.
879769	If the firewall session is in check-new mode, FortiOS will not flush its NPU offload entry when there is a MAC address update of its gateway.
881060	Host Tx dropped counter incrementing and connections failing when throughput reaches 40Gbps.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System* > *Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
884970	Unbalanced throughput on LAG members with LAG enhancement feature enabled.
885823	Sensor showing Temperature 0.00 C.
885837	Traffic dropped as the matching SessionID is being deleted from session table in 20 seconds.
887268	Unable to configure `dscp-based-priority` when `traffic-priority dscp` is configured under `system global`.
891165	Auto-script causes FortiGate to repeat commands.
892195	LAG interface has `NOARP` flag after interface settings change.
892274	Daylight saving time is not applied for Cairo time zone.
893305	Interface could not be brought up if it was part of a virtual switch.
894202	Incorrect temperature calculation appears in sensor list on FG-8xF, FWF-8xF, FG-9xE, FG-10xE, FG-20xE, and FG-14xE.
894884	FSTR session ticket zero causes a memory leak.
895967	FortiGate 1801F in transparent mode cannot reply to an SNMP query.
897905	IPv6 addresses configured on emac-vlan interfaces showing FTP flag after upgrade.
900670	QSFP/QSFP+ port23/port24 are down after upgrading to 7.0.11 on FG-3401E.
903049	`exec sensor list` has blank lines in output.

Bug ID	Description
904414	Port speed 1000auto could not link up with a Cisco switch.
904485	The crashlog might show a Node.JS restarted error, `Failed to fetch web-ui.node-exports: Error: connect ECONNREFUSED`, if the HTTPSD is being killed during conserve mode, stuck in some API calls, or slow response during system super busy.
904486	The FortiGate may display a false alarm message and subsequently initiate a reboot.
906964	DST changes not reflected for timezone 16. The dates are incorrect on the DST for this specific timezone (Santiago-Chile).
907339	dnsproxy process abort due to stack buffer overflow was detected upon function return.
909225	ISP traffic is failing with the LAG interfaces on upstream.
910269	The out of memory killer will generate a kernel panic when memory is very low.
910273	*Last reboot reason: power cycle* after rebooting due to a kernel panic is misleading.
910616	When a non-zero DSCP copied from ingress to egress packet for NAT64, the IP checksum is calculated incorrectly.
910677	Transparent mode FortiGate does not reply to SYN ACK when communicating with FortiManager.
910700	Ports are flapping and down on the FortiGate 3980E.
911396	High system CPU and multiple daemons enter D state on the FortiGate 4401F.
913355	GUI and CLI time mismatch for Mexico Time Zone.
917029	DNS does not respond to short name queries.
920085	DNSproxy CPU is running at 99% on all blades.
922458	Configuration backup does not work well with an account using `mnt read`.
922920	When performing `factoryreset2`, the IP addresses on "a" and "b" are set to default.
922965	hasync daemon high CPU when the session count is large.
922982	FortiGate does not respond to ARP requests for the IP address on the WAN port when the interface is configured as EMAC.
923364	System goes into halt state with `Error: Package validation failed...` message in cases where there are no engine files in the FortiGate when the BIOS security level is set to 2.
923834	The DSL modem on the firewall does not work after the device starts.
924395	IPv6 Local-In ping6 to management interface failed when newly configured.
924654	MAC flapping on switch when UDP packets passthrough VWP multiple times with ASIC offload.
925657	After a manual system administrator password change, the updated `password-expire` is not received by the FortiManager auto-update.
925966	Diagnose sniffer filter blank/empty "" and " " not working.
926035	On D-series FortiGates, a false alarm during system integrity check failure causes the firewall to reboot.

Bug ID	Description
926817	Review the Temperature Sensor for SOC4 system.
928858	Traffic over vpn-id-ipip tunnel blocked when npu-offload is disabled in VPN phase1-interface and the policy has UTM enabled.
929821	httpsd and newcli segmentation fault when trying to generate a TAC Report from GUI and CLI, respectively.
929904	When L3 or L4 hashing algorithm is used, traffic is not forwarded over the same aggregate member after being offloaded by NP7.
935562	NAT port is out-of-range, causing PBA index to be out-of-range.
937887	Unable to load SNMP page with SSO Admin.
939411	Multiple spawns of Hotplug process consuming high CPU resources.
940571	High memory usage, with SLAB consuming the most.
942502	Kernel panic occurs when creating EMAV VLAN interfaces based on an aggregate interface with new kernel 4.1.9.

User & Authentication

Bug ID	Description
794477	When a user's membership in AD or port range is changed, all of the user sessions are cleared.
850473	SSL VPN and firewall authentication SAML does not work when the application requires SHA-256.
854114	Some embedded SSL certificates entered the `Error` state after enable fips-cc.
858877	Dynamic address only has 100 IP addresses while FSSO group lists all 56K ACI endpoints.
865487	Fortinet_GUI_Server certificate auto-regenerates every day.
872814	The SAML assertion is truncated in samld when the payload size is huge.
883006	Adding a new group membership to an FSSO user terminates all the user's open sessions.
899852	FortiGate is sending Class(25) AVP with wrong length in RADIUS accounting when using 2FA with PUSH or external tokens.
900591	When generating guest users according to the settings in the Guest Group, the expiration time of guest users will automatically add an extra 2 hours.
901743	An Error condition occurs during the processing of the UDP packets when device identification is activated on an interface.
915192	Device detection sometimes does not identify the correct IP addresses of devices.
922345	CA bundle (CRDB) to support DigiCert second-generation (G2) full CA and Intermediate CA chain.
923164	EAP proxy daemon may keep reloading after updating the certificate bundle.

Bug ID	Description
936493	Fas daemon crashing on FortiGate.
939517	On the *System* > *Replacement Messages* page, the guest user email template format is not correct when saved/restored to default.
943087	Guest management users no longer view the password automatically generated by the firewall.

VM

Bug ID	Description
901920	AWS external-account-list supports regional endpoints.
913696	In the periodic status check of the OCI VM status, too many API calls caused a lot of 429 errors.
916027	Copy of files between a physical server and Windows Server is slow.
918818	Traffic drops in FortiGate HA A-A, AutoScale in Azure.
924689	FortiGate VMs in an HA cluster deployed on the Hyper-V platform may get into an unresponsive state where multiple services are impacted: GUI management, CLI commands, SSL VPN sessions, DHCP assignment, traffic throughput, and reboot function.
927323	Event log alert `Write Permission Violation` to readonly file on VMware after taking snapshot.
928952	VPN errors after upgrade: Malformed Packets, AUTHENTICATION_FAILED messages, and INVALID_KE_PAYLOAD.
933003	FortiGate-VM KVM with MLX5 not responding to ARP in RHEL environment.
935086	VLAN interface is not reachable on FortiGate-VM running on KVM with SR-IOV interface.

VoIP

Bug ID	Description
887384	SIP session is dropped by ALG with `media type doesn't match` message.

Web Application Firewall

Bug ID	Description
939380	WAF HTTP Method policy does not function correctly.

Web Filter

Bug ID	Description
873086	In a policy-based VDOM, changes are not applied when adding an external threat feed category in the *URL Category* field.
887699	The webfilter admin override entry with expiry time in DST is one hour off in the GUI display.
916140	An error condition occurs in WAD caused by the mismatch between the SNI host and CNAME.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (500+) and large number of WiFi clients (5000+), the *Managed FortiAP* page and *FortiAP Status* widget in the GUI can take a long time to load. This issue does not impact FortiAP operation.
875382	When accessing the Managed FortiAP/Switch view with a large number of devices in the topology, the page would take a long time to load.
877609	RADIUS COA does not work in some cases.
891804	After initial packets, FG-101F stops forwarding wired traffic over FAP-23JF LAN tunneled with a dynamic VLAN VAP.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models.
905406	In `auth-logon` and `auth-logout` logs, Wi-Fi users with random public IP addresses are observed.
920189	Intermittent behavior in Hostapd caused by enabling/disabling `fast-bss-transition`.
921456	FAP-431F is deauthenticating clients after roaming when DHCP enforcement is enabled on the SSID, even when the client gets IP from DHCP.
926676	Enable DFS channels on wtp-profile for FortiAP 431G and FortiAP 433G in region A/S/N(No-Brazil).
944465	On the *WiFi & Switch Controller* > *Managed FortiAPs* page of a non-management VDOM, the *Register* button is unavailable in the *Device Registration* pane.
945356	FortiOS fails to get all of the configured MAC ACL entries.

ZTNA

Bug ID	Description
889994	After client device info is updated, the session is closed even though all information from the session still matches the policy.
923804	ZTNA logs are showing the log message `Denied: failed to match a proxy-policy` when client device information matches the policy.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
854906	FortiOS 7.2.6 is no longer vulnerable to the following CVE Reference: • CVE-2023-45862
914808	FortiOS 7.2.6 is no longer vulnerable to the following CVE Reference: • CVE-2023-37930
948163	FortiOS 7.2.6 is no longer vulnerable to the following CVE Reference: • CVE-2023-42785
948164	FortiOS 7.2.6 is no longer vulnerable to the following CVE Reference: • CVE-2023-42786

Known issues

The following issues have been identified in version 7.2.6. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Explicit Proxy

Bug ID	Description
877337	HTTPS requests over IPv6 are not matched sometimes to the proxy policy when the IPv6 Internet Service Database is applied in the proxy policy.

894557	In some cases, the explicit proxy policy list can take a long time to load due to a delay in retrieving the proxy statistics. This issue does not impact explicit proxy functionality.
	Workaround: restart the WAD process, or update the number of WAD processors.
	`config system global`
	`  set wad-worker-count <integer>`
	`end`

FortiGate 6000 and 7000 platforms

Bug ID	Description
885205	IPv6 ECMP is not supported for the FG-6000F and FG-7000E platforms. IPv6 ECMP is supported for the FG-7000F platform.
887946	UTM traffic is blocked by an FGSP configuration with asymmetric routing.
892499	IPv6 SD-WAN service rules are not supported on 6KF and 7KE models. 7KF models are not impacted.
906481	The GUI becomes unresponsive, and sometimes may work after rebooting.
907695	The FortiGate 6000 and 7000 platforms do not support IPsec VPN over a loopback interface or an NPU inter-VDOM link interface.
909163	Local logging support is needed on all SLBC models.
910883	The FortiGate 6000s or 7000s in an FGSP cluster may load balance FTP data sessions to different FPCs or FPMs. This can cause delays while the affected FortiGate 6000 or 7000 re-installs the sessions on the correct FPC or FPM.
911244	FortiGate 7000E IPv6 routes may not be synchronized correctly among FIMs and FPMs.

Bug ID	Description
937879	FortiGate 7000F chassis with FIM-7941Fs cannot load balance fragmented IPv6 TCP and UDP traffic. Instead, fragmented IPv6 TCP and UDP traffic received by the FIM-7941F interfaces is sent directly to the primary FPM, bypassing the NP7 load balancers. IPv6 ICMP fragmented traffic load balancing works as expected. Load balancing fragmented IPv6 TCP and UDP traffic works as expected in FortiGate 7000F chassis with FIM-7921Fs.

941944	CPU usage data displayed on the FortiGate 6000 GUI is actually CPU usage data for the management board. CPU usage data displayed on the FortiGate 7000 GUI is actually the CPU usage for the primary FIM.
	Use the global `get system performance status` command to display CPU usage and other performance information for all components (on the FortiGate 6000 the management board and all FPCs, or on the FortiGate 7000 the FIMs and FPMs).
	This command also displays global performance information including:
	`Dataplane CPU states: 1%`
	`Dataplane memory states: 21%`
	`Dataplane average sessions: 8720 sessions in 1 minute`
	`Dataplane average session setup rate: 4632 sessions per second in last 1 minute`

948388	On the FortiGate 6000s, missing image update command in the CLI: `execute load-balance update image`.
948750	When EMAC-VLAN interfaces are removed from the configuration while in operation on FortiGate 7000F series devices, TCP traffic through their underlying VLAN interfaces fails.
949175	On the FortiGate 7121F, with FIM2 as the master FIM, making FIM1 the master causes NP7 PLE invalidation.
949240	SLBC special ports will not match local-in policy in the management path.
951135	Graceful upgrade of a FortiGate 6000 or 7000 FGCP HA cluster is not supported when upgrading from FortiOS 7.0.12 to 7.2.6. Upgrading the firmware of a FortiGate-6000 or 7000 FGCP HA cluster from 7.0.12 to 7.2.6 should be done during a maintenance window, since the firmware upgrade process will disrupt traffic for up to 30 minutes. Before upgrading the firmware, disable `uninterruptible-upgrade`, then perform a normal firmware upgrade. During the upgrade process the FortiGates in the cluster will not allow traffic until all components (management board and FPCs or FIMs and FPMs) are upgraded and both FortiGates have restarted. This process can take up to 30 minutes.
954881	Image synchronization failure happened after a factory reset on FortiGate 7000E/F .

GUI

Bug ID	Description
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.
946943	On FortiGate 6000F series devices, the WiFi & Switch controller should not be available in the management VDOM on SLBC devices.

Hyperscale

Bug ID	Description
802182	After successfully changing the VLAN ID of an interface from the CLI, an error message similar to `cmdb_txn_cache_data(query=log.npu-server,leve=1) failed` may appear.
817562	NPD/LPMD cannot differentiate the different VRF's, considers as VRF 0 for all.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
853258	Packets drop, and different behavior occurs between devices in an HA pair with ECMP next hop.
872146	The `diagnose sys npu-session list` command shows an incorrect policy ID when traffic is using an intra-zone policy.
920228	NAT46 NPU sessions are lost and traffic drops when a HA failover occurs.
949188	With NAT64 HS policy, ICMP reply packets are dropped by FortiOS.
950582	Traffic not passing across the VDOM link.

IPsec VPN

Bug ID	Description
916260	The IPsec VPN tunnel list can take more than 10 seconds to load if the FortiGate has large number of tunnels, interfaces, policies, and addresses. This is a GUI display issue and does not impact tunnel operation.

Log & Report

Bug ID	Description

932537	If Security Rating is enabled to run on schedule (every 4 hours), the FortiGate can unintentionally send local-out traffic to fortianalyzer.forticloud.com during the Security Rating run.
	Workaround: disable on-schedule Security Rating run:
	`config system global`
	`    set security-rating-run-on-schedule disable`
	`end`

Proxy

Bug ID	Description
837724	Unhandled error condition found on WAD.

Routing

Bug ID	Description
903444	The `diagnose ip rtcache list` command is no longer supported in the FortiOS 4.19 kernel.

SSL VPN

Bug ID	Description
795381	FortiClient Windows cannot be launched with SSL VPN web portal.
947210	Application sslvpnd `*** code requested backtrace ***` was observed during graceful upgrade.

System

Bug ID	Description
887940	Status light is not showing on the FortiGate 60F or 100F after a cold reboot.

Upgrade

Bug ID	Description
939011	On the Fortigate 6000F, the ALL TP VDOM cannot synchronize because of `switch-controller.auto-config.policy`.

Web Filter

Bug ID	Description
885222	HTTP session is logged as HTTPS in web filter when VIP is used.

WiFi Controller

Bug ID	Description
869106	The layer 3 roaming feature may not work when the wireless controller is running multiple cw_acd processes (when the value of `acd-process-count` is not zero).
869978	CAPWAP tunnel traffic over tunnel SSID is dropped when offloading is enabled.
873273	The *Automatically connect to nearest saved network* option does not work as expected when FWF-60E client-mode local radio loses connection.
903922	Physical and logical topology is slow to load when there are a lot of managed FortiAP (over 50). This issue does not impact FortiAP management and operation.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

www.fortinet.com